

kvmadmin - KVM-via-IP Admin Tool

The kvmadmin.exe command-line tool can be used to perform various administrative tasks on a KVM-via-IP unit remotely via the VNC protocol. To perform these tasks you will need to know the IP address of the unit and be able to log on as the admin user. The program is invoked as:

```
kvmadmin <command> <ip-address> [<parameters>]
```

where <command> is one of:

```
-setconfig <config-file>  
-getconfig <config-file>  
-setusers <csv-file>  
-getlog <log-file>  
-gethosts <csv-file>  
-sethosts <csv-file>  
-setmodes <csv-file>  
-getidhash <text-file>  
-reboot
```

Connecting to the unit with the kvmadmin tool is essentially the same as with an ordinary VNC viewer, except that no graphical interface is provided. Once a connection is established you will be prompted for the admin user's password. Alternatively it may be specified as a parameter directly on the command line, e.g.:

```
kvmadmin -getlog log.txt 192.168.2.1 -password=mypassword
```

A better way of avoiding the need to type the admin password each time is to use a [ticket](#).

As with the normal viewer, kvmadmin checks the unit's identity to protect against spoofing and man-in-the-middle attacks. It will display a warning on the console requiring the user to type 'y' or 'n' to accept a unit's signature for the first time, or if the unit's signature has changed for any reason.

There are two ways of avoiding this interaction by using command-line arguments. **If you are sure that your network is 100% safe** then you can disable this behaviour by specifying the "-verifyid=0" parameter, e.g.:

```
kvmadmin -getlog log.txt 192.168.2.1 -verifyid=0
```

A more secure alternative is to specify a short hash of the unit's expected signature using the "-idhash" parameter, e.g.:

```
kvmadmin -getlog log.txt 192.168.2.1 -idhash=48b4fd080714af32
```

You can obtain such a hash using the ["-getidhash" command](#).

Saving and restoring the unit's configuration

The configuration settings of a unit can be downloaded to a file using the "-getconfig" command, e.g.:

```
kvmadmin -getconfig kvm1.cfg 192.168.2.1
```

This will store the settings in the file "kvm1.cfg". To upload these settings to a unit, use the "-setconfig" command, e.g.:

```
kvmadmin -setconfig kvm1.cfg 192.168.2.2
```

After setting the configuration on a unit remotely it is best to perform a remote reboot using the "-reboot" command in order to ensure that the new settings have taken effect.

Note that for security reasons the unit will not allow the user names and passwords to be downloaded so they cannot be transferred from one unit to another by this mechanism. If you wish to use the same set of user names and passwords on more than one unit then you can put them into a CSV file and set them on the unit via the "-setusers" command (see below).

Setting user names and passwords

The "-setusers" command can be used to set the user names and passwords on the unit. The user names should be stored in a ".csv" file such as can be generated by Microsoft Excel, or alternately created by hand via Notepad or your favourite editor.

To apply the file "users.csv" to the unit 192.168.2.1:

```
kvmadmin -setusers users.csv 192.168.2.1
```

Each line in the CSV file represents a user on the unit. There may be up to sixteen users. Each line should have three entries, the first being the user name, the second being the new password for that user, and the third specifying the access rights - any combination of the letters L, M, R and P, corresponding to "Local", "Modem", "Remote" and "Power" settings respectively.

Note that the name of the first user should always be "admin" and its access rights should always be "LMRP" (in fact the unit will enforce this by ignoring the specified values).

The following example "users.csv" file sets the new admin password to "newadminpasswd" and creates two users, "bert" and "ernie" with the passwords "passwd1" and "passwd2" respectively, with slightly different access rights:

```
admin,newadminpasswd,LMRP
bert,passwd1,LMR
ernie,passwd2,LR
```

Optionally, the first two lines of the file can instead be used to specify the user name and password used to connect to the unit. The first line should have "admin" in the first field, followed by empty second and third fields. The second line should have the current admin password in the first field, again followed by empty second and third fields. The third line onwards should then be as before, e.g.:

```
admin, ,  
oldadminpasswd, ,  
admin,newadminpasswd,LMRP  
bert,passwd1,LMR  
ernie,passwd2,LR
```

It goes without saying that the contents of such a file are sensitive and appropriate care should be taken. The users specified always replace any existing users on the unit.

Note that Microsoft Excel will not allow you to save a field in a CSV file which start with certain characters ("+", "-", "=", "@", ""). If a password begins with such a character, prefix it with a space; this will be stripped off before being sent to the unit. Equally if the password begins with a space it must be prefixed by another space which will be stripped off.

Getting the event log

The event log can be retrieved from a unit via the "-getlog" command. For example, to get the event log from unit 192.168.2.1 into the file log.txt, issue the command:

```
kvmadmin -getlog log.txt 192.168.2.1
```

The log file is a plain text file, in the same form as it appears in the "Logging and Status" page of the remote configuration menus.

Getting and setting host configuration

The "-gethosts" command can be used to retrieve all of the settings corresponding to multiple hosts connected to the unit via one or more KVM switches, e.g.:

```
kvmadmin -gethosts hosts.csv 192.168.2.1
```

Each line in the CSV file represents a host. The first five fields are the host name, users, hotkeys, power on and power off sequences (the same as in the "Host Configuration" dialog in the remote configuration menus). Note that the users field must be "*" to allow all users - an empty string means no-one is allowed access to the host. The last two fields contain the internal representation of the mouse and video calibration settings.

Note again that because of Microsoft Excel's restrictions on CSV files, some fields may need an extra space on the front, in particular the hotkeys field which normally starts with a "+".

To set the host configuration on a unit from a CSV file, use the "-sethosts" command, e.g.:

```
kvmadmin -sethosts hosts.csv 192.168.2.2
```

The CSV file can either be one downloaded from a unit, or created by hand for a particular installation. When creating a hosts file, the first three fields are required, the rest are optional. For example, the following might be used where the unit is connected to a simple 4-port switch:

```
Computer 1,*, +ctrl+alt+1
Computer 2,*, +ctrl+alt+2
Computer 3,*, +ctrl+alt+3
Computer 4,*, +ctrl+alt+4
```

As with the users CSV file, the first two lines of the file can optionally be used to specify the user name and password used to connect to the unit. The first line should have "admin" in the first field, followed by empty second and third fields. The second line should have the current admin password in the first field, again followed by empty second and third fields. The third line onwards should then be as before.

Setting custom video modes

The "-setmodes" command can be used to set the timing parameters of custom video modes. This is an advanced feature that should only be used by an expert who understands monitor timings in detail.

Again a CSV file is used. Each line represents a video mode, and consists of 12 fields. The first field is the name by which the mode is identified on the "Info" dialog. The second field is the pixel clock frequency in MHz.

The next four fields are the horizontal timings in pixels, being the displayed width, the horizontal front porch, the horizontal sync width, and the horizontal back porch. The sum of these is the total horizontal width in pixels - so dividing the pixel clock frequency by this value should give the horizontal sync frequency. Conventionally, all of these numbers are multiples of 8.

The following four fields are the equivalent vertical timings in lines - the displayed height, the vertical front porch, vertical sync width and the vertical back porch. The sum of these is the total number of lines in a frame - dividing the horizontal sync frequency by this value should give the vertical refresh frequency.

The final two fields are the horizontal and vertical sync polarities respectively, being 0 for negative polarity, 1 for positive polarity.

For example, the following are the timings for a 1280x768 mode which would otherwise be detected as the standard VESA 1024 x 768 @ 60Hz mode built into the unit (these two can be distinguished only by their polarities):

```
custom 1280 x 768 @ 60Hz, 80.14, 1280, 64, 136, 200, 768, 1, 3, 23, 0, 1
```

Getting a hash of the unit's signature

The "-getidhash" command gets a 64-bit hash of the unit's signature. It stores the resulting 16 hex digits as a single line in a text file. Once the hash has been obtained it can be provided to invocations of the VNC viewer or kvmadmin itself via the "-idhash" parameter. This allows for protection from man-in-the-middle attacks on untrusted networks while avoiding the need for the warning dialogs normally displayed when a unit's signature is unknown or has changed.

Rebooting the unit

A remote reboot of the unit can be performed using the "-reboot" option, e.g.:

```
kvmadmin -reboot 192.168.2.1
```

The unit should be back after approximately ten seconds. Any other connections to the unit will be dropped.

Using Tickets

Tickets are designed for allowing secure connections to a unit without the need for a password. The kvmadmin tool can be passed a ticket on the command-line via the "-ticket" option. Tickets can be generated with the [ticketgen](#) program. The ticket must be for the "admin" user and must not have expired or be otherwise invalid.